IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA
CENTRAL DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. LI SHAOMING, MO HAILONG, a/k/a Robert Mo, WANG LEI, WANG HONGWEI, YE JIAN, LIN YONG and MO YUN, Defendants.	Criminal No. 4:13-cr-147 **BRIEF IN SUPPORT OF MOTION FOR DISCLOSURE OF FISA APPLICATIONS, ORDERS, AND RELATED MATERIALS**

As detailed in Mr. Mo's motion to suppress FISA-derived evidence, FISA generally permits the government – under specified circumstances and procedures – to obtain "foreign intelligence information" concerning certain activities of "foreign powers" and "agents of foreign powers." Here, the government convinced the FISC to authorize FISA surveillance of employees of privately-owned United States and Chinese agricultural companies who were suspected of stealing corn germplasm from privately-owned United States agricultural companies. The case has nothing to do with "foreign intelligence information," and neither Mr. Mo nor any other potential target of the surveillance was a "foreign power" or an "agent of a foreign power."

The critical question, therefore, is how the government convinced the FISC to approve FISA surveillance of Mr. Mo and others. It is highly likely that whatever the government told the FISC on the "foreign power," "agent of a foreign power," and "foreign intelligence information" issues was either materially false or had material omissions. For example, to the

extent the government represented to the FISC that DBN – the Chinese agricultural company for which Mr. Mo works – was directed and controlled by the PRC government, that representation was false, as demonstrated in Mr. Mo's motion to suppress FISA information, which he is filing with this motion. Similarly, the government's certification that the information sought could not reasonably be obtained through "normal investigative techniques" likely rested on material falsehoods or omissions, given the vast range of investigative techniques that the government successfully employed in its investigation.

Without access to the underlying applications, orders, and related materials (affidavits accompanying the applications, for example), the defense can only speculate; we cannot identify specific falsehoods or omissions to make the "substantial preliminary showing" that *Franks v. Delaware*, 438 U.S. 154 (1978), requires for an evidentiary hearing. *Id.* at 155-56. As Judge Ilana Rovner recently acknowledged, "Thirty-six years after the enactment of FISA, it is well past time to recognize that it is virtually impossible for a FISA defendant to make the showing that *Franks* requires in order to convene an evidentiary hearing." *United States v. Daoud*, 755 F.3d 479, 496 (7th Cir. 2014) (Rovner, J., concurring), *cert. denied*, 2015 U.S. LEXIS 1309 (U.S. Feb. 23, 2015). Nor can we show concretely that the government's certifications concerning "foreign intelligence information" and the necessity for the FISA surveillance are clearly erroneous.

As Judge Rovner recognized, the Court "cannot conduct more than a limited *Franks* review on its own." *Id.* Without assistance from the defense, the Court lacks the investigative resources and knowledge of the facts necessary to make the *Franks* determination or to assess the certifications. For these reasons, disclosure of the applications, orders, and related materials is "necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §

1806(f). Disclosure is also required as a matter of due process under the three-part standard of *Mathews v. Eldridge*, 424 U.S. 319 (1976), and under *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny.

ARGUMENT

When an "aggrieved person" such as Mr. Mo moves to suppress the fruits of FISA surveillance, the court must review the FISA application, order, and related materials *ex parte* and *in camera*, unless "disclosure [to the defendant] is necessary to make an accurate determination of the legality of the surveillance," 50 U.S.C. § 1806(f), or unless disclosure is required as a matter of due process, *id.* § 1806(g).[1]

As we demonstrate below, the Court should order disclosure of the underlying FISA materials. Part I.A. shows that disclosure is "necessary" under § 1806(f) when it would substantially promote an accurate determination of legality. Part I.B. demonstrates that, under the unusual circumstances of this case, disclosure would substantially promote an accurate determination of Mr. Mo's *Franks* challenge and his contention that the government's certifications concerning "foreign intelligence information" and the necessity for the FISA surveillance are clearly erroneous. Part II shows that disclosure is required as a matter of Due Process under the well-established *Mathews* standard and under *Brady*.

The government will argue, as it invariably does, that in the 36-year history of FISA, only one district court has ever ordered disclosure of FISA materials, and it was reversed. *See United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014) (reversing disclosure order), *cert. denied*, 2015 U.S. LEXIS 1309 (U.S. Feb. 23, 2015). But Congress plainly intended that disclosure would

[1] The Court's obligation to conduct *ex parte*, *in camera* review is triggered when the Attorney General files an affidavit that "disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). The Attorney General has filed such an affidavit in every FISA case to date, and we assume that an affidavit will be filed here.

occur in a significant number of cases, and this is precisely the kind of case it had in mind. The Court should reject the government's suggestion that it reflexively follow what other courts have done in other cases under other circumstances.

I. DISCLOSURE IS "NECESSARY" UNDER 50 U.S.C. § 1806(f) BECAUSE IT WOULD SUBSTANTIALLY PROMOTE AN ACCURATE DETERMINATION OF LEGALITY.

The legislative history and statutory purposes of 50 U.S.C. § 1806(f) demonstrate that disclosure is "necessary" under § 1806(f) when it would substantially promote an accurate determination of legality. Under the circumstances of this case, that standard is met; disclosure would substantially promote an accurate determination of Mr. Mo's *Franks* challenge and of his contention that the government's certifications concerning "foreign intelligence information" and the necessity for FISA surveillance are clearly erroneous.

A. The Word "Necessary" in 50 U.S.C. § 1806(f) Means That Disclosure Would Substantially Promote an Accurate Determination of Legality.

As the D.C. Circuit has observed, "The term 'necessary' is a chameleon-like word whose meaning . . . may be influenced by its context . . . .[It] is not language of plain meaning." *Cellco Partnership v. FCC*, 357 F.3d 88, 96-97 (D.C. Cir. 2004)). The "context" of § 1806(f), including its legislative history and the purposes of FISA, demonstrates that Congress intended courts to order disclosure when defense access to the underlying FISA materials would substantially promote the accuracy of the court's determination of legality.

1. Courts Routinely Interpret "Necessary" To Mean Something Less Than Essential or Indispensable.

Courts have frequently interpreted "necessary" to mean "less than absolutely essential, and have explicitly found that a measure may be 'necessary' even though acceptable alternatives have not been exhausted." *CT&IA v. FCC*, 330 F.3d 502, 510 (D.C. Cir. 2003) (quotation

omitted). Most famously, the Supreme Court confronted the term "necessary" in 1819, when it first interpreted the Necessary and Proper Clause. That provision gives Congress the power

> [t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.

U.S. Const. art. I, § 8. In defining the contours of the Clause, Chief Justice Marshall emphasized that "necessary" does not mean "absolutely necessary." *McCulloch v. Maryland*, 17 U.S. (4 Wheat) 316, 413-14 (1819); *see also, e.g., Jinks v. Richland County*, 538 U.S. 456, 462 (2003) ("[W]e long ago rejected the view that the Necessary and Proper Clause demands that an Act of Congress be absolutely necessary to the exercise of an enumerated power.") (quotation omitted)). Similarly, in *Commissioner v. Tellier*, 383 U.S. 687 (1966), the Court found that the word "necessary" in the phrase "ordinary and necessary [business] expenses" imposes "only the minimal requirement that the expense be appropriate and helpful for the development of the taxpayer's business." *Id.* at 689 (quotations and brackets omitted).

Cases interpreting "necessary" emphasize that its meaning must be "harmonized with its context." *Armour & Co. v. Wantock*, 323 U.S. 126, 130 (1944). Relying on context, courts have often found "necessary" to mean something closer to "helpful" than to "essential" or "indispensable." *See, e.g., Snider v. United States*, 468 F.3d 500, 513 (8th Cir. 2006) (interpreting "necessary" in 26 U.S.C. § 6103; court rejects "strictly essential" and holds that the "'appropriate or helpful' meaning of 'necessary' is the only practical interpretation in this context"); *Prometheus Radio Project v. FCC*, 373 F.3d 372, 393-94 (3d Cir. 2004) (interpreting "necessary" in § 202(h) of the Telecommunications Act of 1996 to mean "'convenient,' 'useful,' or 'helpful,' not 'essential' or 'indispensable'"); *FTC v. Rockefeller*, 591 F.2d 182, 188 (2d Cir. 1979) (interpreting "necessary" in 15 U.S.C. § 46; court holds that FTC's authority to conduct an ancillary investigation of a bank when "necessary" did not require investigation to be "absolutely

needed" or "inescapable," but instead that it "arise reasonably and logically out of the main investigation").

These cases confirm that the word "necessary" in § 1806(f) must be read in light of the legislative history of FISA and the statutory purpose. These interpretive aids confirm that, in this context, "necessary" means that disclosure would substantially promote the accuracy of the court's determination of legality.

2. The Legislative History of FISA Shows That Congress Intended Disclosure When It Would Substantially Promote Accurate Determination of Legality.

Two authoritative Senate Reports – one from the Senate Judiciary Committee and the other from the Senate Intelligence Committee – discuss in detail the provision that became § 1806. The Reports observe:

> The extent to which the government should be required to surrender to the parties in a criminal trial the underlying documentation used to justify electronic surveillance raises delicate problems and competing interests. On the one hand, broad rights of access to the documentation and subsequent intelligence information can threaten the secrecy necessary to effective intelligence practices. However, the defendant's constitutional guarantee of a fair trial could seriously be undercut if he is denied the materials needed to present a proper defense. The Committee believes that a just, effective balance has been struck in this section.

S. Rep. 604(I), 95th Cong., 1st Sess. 53, *reprinted in* 1978 U.S.C.C.A.N. 3904, 3954; *see* S. Rep. 701, 95th Cong., 1st Sess. 59 (similar passage in Senate Intelligence Committee Report), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4028. Turning to § 1806(f), the Committees summed up the disclosure provision as follows:

> The committee views the procedures set forth in this subsection as striking a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.
>
> The decision whether it is necessary to order disclosure to a person is for the Court to make after reviewing the underlying documentation and determining

> its volume, scope and complexity. The committee has noted the reasoned discussion of these matters in the opinion of the Court in United States v. Butenko, [494 F.2d 593 (3d Cir. 1974) (en banc)]. There, the Court, faced with the difficult problem of determining what standard to follow in balancing national security interests with the right to a fair trial stated:
>
> "The distinguished district court judge reviewed in camera the records of the wiretaps at issue here before holding the surveillances to be legal . . . Since the question confronting the district court as to the second set of interceptions was the legality of the taps, not the existence of tainted evidence, it was within his discretion to grant or deny Ivanov's request for disclosure and a hearing. The exercise of this discretion is to be guided by an evaluation of the complexity of the factors to be considered by the court and by the likelihood that adversary presentation would substantially promote a more accurate decision." (494 F.2d at 607.)
>
> Thus, in some cases, the Court will likely be able to determine the legality of the surveillance without any disclosure to the defendant. In other cases, however, the question may be more complex because of, for example, indications of possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which includes [sic] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order. In such cases, the committee contemplates that the court will likely decide to order disclosure to the defendant, in whole or in part since such disclosure "is necessary to make an accurate determination of the legality of the surveillance." [Footnote omitted.]
>
> Cases may arise, of course, where the Court believes that disclosure is necessary to make an accurate determination of legality, but the Government argues that to do so, even given the Court's broad discretionary power to excise certain sensitive portions, would damage national security. In such situations the Government must choose – either disclose the material or forego the use of the surveillance-based evidence. Indeed, if the Government objects to the disclosure, thus preventing a proper adjudication of legality, the prosecution would probably have to be dismissed . . . .

S. Rep. 604(I), *supra*, at 58-59 (footnote omitted; ellipsis in original), *reprinted in* 1978 U.S.C.C.A.N. at 3959-60; *see* S. Rep. 701, *supra*, at 64-65 (identical language in Senate Intelligence Committee Report), *reprinted in* 1978 U.S.C.C.A.N. at 4033-44.

Several points are evident from this passage. First, the Senate Judiciary and Intelligence Committees plainly did not intend to erect an insuperable barrier to disclosure. To the contrary,

in choosing a balanced approach, the Committees specifically eschewed "an entirely in camera proceeding."

Second, the Committees, through their citation to *Butenko*, placed broad discretion in district judges in determining when disclosure is "necessary to make an accurate determination of the legality of the surveillance."

Third, the Committees – again through their reliance on *Butenko* – suggest that the "necessary" standard is met when the district court determines that "adversary presentation would substantially promote a more accurate decision."

Fourth, the Committees noted the district court's "broad discretionary power to excise certain sensitive portions" from the FISA materials before disclosure. This recognition of the district court's inherent power to take necessary protective measures finds a statutory basis both in § 1806(f) itself and in CIPA (discussed below). That power substantially ameliorates any national security concerns.

Finally, the Senate Judiciary and Intelligence Committees contemplated – and did not shy away from – the possibility that the court would order disclosure, the government would refuse to comply, and the court would suppress the surveillance or dismiss the prosecution. Just as Congress did in CIPA, 18 U.S.C. App. 3 § 6(e), the Committees left the choice with the government: either comply with the disclosure order or refuse and suffer appropriate sanctions.

Two other portions of the legislative history are relevant as well. First, an early version of the definition of "foreign intelligence information" included the words "necessary" and "essential." "Necessary," according to the Senate Judiciary Committee, "requires more than a showing that the information would be useful or convenient." S. Rep. 604(I), *supra*, at 31, *reprinted in* 1978 U.S.C.C.A.N. at 3933. "Essential" requires "a showing that the information is

important and required but not that it is of utmost importance or indispensable." *Id.* Thus, "necessary" merely meant something more than "useful or convenient," and not even "essential" required a showing that information was "indispensable."

The Senate Intelligence Committee deleted "essential" from the final definition of "foreign intelligence information" (codified at 50 U.S.C. § 1801(e)). The Intelligence Committee declared that by the term "necessary," it "intends to require more than a showing that the information would be useful or convenient. The committee intends to require that the information is both important and required. The use of this standard is intended to mandate that a *significant need* be demonstrated by those seeking the surveillance." S. Rep. 701, *supra*, at 31 (emphasis added), *reprinted in* 1978 U.S.C.C.A.N. at 4000.

Second, the minimization procedures in 50 U.S.C. § 1801(h)(2) bar dissemination of nonpublicly available information in a manner that identifies any United States person without the person's consent, "unless such person's identity is necessary to understand foreign intelligence information or assess its importance." The House Conference Report explains that "[b]y 'necessary' the conferees do not mean that the identity must be essential to understand the information or assess its importance. The word necessary requires that a knowledgeable intelligence analyst make a determination that the identity will contribute in a meaningful way to the ability of the recipient of the information to understand the information or assess its importance." H. Conf. Rep. 1720, 95th Cong., 2d Sess. 23 (Oct. 5, 1978).

The use of "necessary" in §§ 1801(e) and 1801(h)(2) sheds light on the word's meaning in § 1806(f). As the Supreme Court has observed, "[I]dentical words and phrases within the same statute should normally be given the same meaning." *Hall v. United States*, 132 S. Ct. 1882, 1891 (2012) (quotation omitted). Under this principle, the meanings ascribed to "necessary" in

§§ 1801(e), 1801(h)(2), and 1806(f) should be the same, absent an indication to the contrary. And, according to the legislative history, the meanings are very similar: "significant need" in § 1801(e), "contribute in a meaningful way" in § 1801(h)(2), and "substantially promote" in § 1806(f).

3. The Legislative Purpose of FISA – To Balance Civil Liberties and National Security – Supports the "Substantially Promotes" Standard.

A court must construe a statutory term "in a manner consistent with the [statute's] purpose." *Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 118 (2001); *see, e.g., Yates v. United States*, 2015 U.S. LEXIS 1503, *15 (U.S. Feb. 25, 2015) (plurality opinion) (looking to "broader context of the statute as a whole" to determine meaning of statutory phrase) (quotation omitted). FISA "was enacted to create a framework whereby the Executive could conduct electronic surveillance for foreign intelligence purposes without violating the rights of citizens."[2] The Act "was intended to strike a sound balance between the need for such surveillance and the protection of civil liberties."[3] Interpreting "necessary" in § 1806(f) to mean "substantially promote" is fully consistent with FISA's effort to balance civil liberties and the need for surveillance.

---

[2] *United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (en banc), *vacated on other grounds*, 543 U.S. 1097 (2005), *reinstated in relevant part*, 405 F.3d 1034 (4th Cir. 2005) (en banc).

[3] *In re Kevork*, 788 F.2d 566, 569 (9th Cir. 1986) (quotation omitted); *see, e.g.,* S. Rep. 604(I), *supra*, at 4 (Senate Judiciary Committee Report notes Attorney General Griffin Bell's view that "this bill strikes the balance, sacrifices neither our security nor our civil liberties, and assures that the abuses of the past will remain in the past . . . ."), *reprinted in* 1978 U.S.C.C.A.N. at 3905-06; *id.* at 7 (bill "goes a long way in striking a fair and just balance between protection of national security and protection of personal liberties"), *reprinted in* 1978 U.S.C.C.A.N. at 3908; *id.* at 9 ("Striking a sound balance between the need for such surveillance and the protection of civil liberties lies at the heart of S. 1566."), *reprinted in* 1978 U.S.C.C.A.N. at 3910; S. Rep. 701, *supra*, at 7, 16 (Senate Intelligence Committee Report with similar remarks), *reprinted in* 1978 U.S.C.C.A.N. at 3975, 3985.

Interpreting "necessary" so strictly that disclosure *never* occurs – the government's preferred approach – does nothing to advance civil liberties. To the contrary, as we discuss in Part II.B. below, a system that operates in secret, with no adversarial input – as the FISA process has functioned for more than 36 years – is almost certain to breed abuse. The stark fact is that the FISA system, interpreted by the courts to require ex parte proceedings in *every* case and *never* to grant defense counsel access to FISA applications and orders, has failed to protect civil liberties. Interpreting § 1806(f) as Congress intended, to permit disclosure when adversarial proceedings will substantially promote the accuracy of the district court's determination, marks an important step toward restoring the balance that Congress sought to strike in 1978.

The government invariably resists disclosure of FISA materials to defense counsel on the ground that *any* disclosure of FISA materials, *ever*, to *any* defense counsel, under *any* circumstances, will cause irreparable damage to national security. The Senate Judiciary and Intelligence Committees did not accept that view in 1978, as their Reports confirm. As we discuss below in Part II.C., the argument is even more clearly wrong now, following the enactment of the Classified Information Procedures Act ("CIPA") in 1980 (two years after the enactment of FISA) and the extensive experience that courts, prosecutors, and defense counsel have had with the statute since then. Through the use of "appropriate security procedures and protective orders," 50 U.S.C. § 1806(f), including the procedures that CIPA provides, the Court can order disclosure in a manner that adequately protects legitimate national security concerns.

B. Disclosure Will Substantially Promote the Accuracy of the Court's Determination of the Legality of the Surveillance.

In three critical respects, disclosure of the underlying FISA applications, orders, and other materials will substantially promote the Court's determination of the legality of the surveillance.

1. Falsehoods and Omissions Concerning "Foreign Power" and "Agent of a Foreign Power."

The government convinced the FISC that there was probable cause to believe that Mr. Mo, or another target of the surveillance that intercepted Mr. Mo's communications, was a "foreign power" or an "agent of a foreign power." As explained in Mr. Mo's motion to suppress, whatever information the government submitted to persuade the FISC on that point was either false or materially incomplete. The declaration of Dr. Tong Yao – attached to the motion to suppress – shows that DBN is a privately-owned and privately-controlled company. The PRC government does not "direct" or "control" DBN. 50 U.S.C. § 1801(a)(6). DBN thus is not a "foreign power," and neither Mr. Mo nor any other employee of DBN is an "agent of a foreign power." Neither Mr. Mo nor any other possible target of the surveillance that intercepted his communications "knowingly engage[d] in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States," or "knowingly aid[ed] or abet[ted] [or conspired with] any person in the conduct of" these activities.[4]

Mr. Mo's motion to suppress challenges the government's applications under *Franks*, on the ground that they contain material falsehoods and omissions. But without access to the underlying applications, defense counsel cannot identify the falsehoods or omissions that led the FISC to find probable cause that the target of the surveillance was a "foreign power" or an "agent of a foreign power." As Judge Rovner has recognized,

> A *Franks* motion is premised on material misrepresentations and omissions in the warrant affidavit; but without access to that affidavit, a defendant cannot identify such misrepresentations or omissions, let alone establish that they were intentionally or recklessly made. As a practical matter, the secrecy shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief

[4] 50 U.S.C. § 1801(b)(2)(A), (E) (ellipses omitted).

> under *Franks* absent a patent inconsistency in the FISA application itself or a *sua sponte* disclosure by the government that the FISA application contained a material misstatement or omission.

Daoud, 755 F.3d at 486 (Rovner, J., concurring). Here, we cannot even determine the *identity* of the target – that is, whether it was Mr. Mo or someone else. The Court, lacking access to the discovery, to the information the defense possesses through its own knowledge and investigation, and to investigative resources, cannot assess on its own whether the applications contain falsehoods, or whether they omit information that would change the probable cause assessment. *Id.* ("[T]he court, which does have access to the application, cannot, for the most part, independently evaluate the accuracy of that application on its own without the defendant's knowledge of the underlying facts.").

Judge Rovner declared that "*Franks* serves as an indispensable check on potential abuses of the warrant process, and means must be found to keep *Franks* from becoming a dead letter in the FISA context." *Id.* Those "means" are readily available here: provide defense counsel access to the FISA applications, orders, and other materials, as Congress intended. There is no other way to ensure an accurate determination of Mr. Mo's *Franks* claim.

2. Certifications Concerning "Foreign Intelligence Information."

The applications to the FISC contained certifications from a high executive branch official that he or she "deem[ed] the information sought to be foreign intelligence information" and that "a significant purpose of the surveillance [was] to obtain foreign intelligence information."[5] In addition, the certifications "designate[d] the type of foreign intelligence information being sought according to the categories described in" 50 U.S.C. § 1801(e) and

[5] *Id.* § 1804(a)(6)(A), (B).

included "a statement of the basis for the certification that . . . the information sought is the type of foreign intelligence information designated."[6]

For the reasons outlined in Mr. Mo's motion to suppress, the information that the FISA surveillance sought to obtain – concerning the alleged theft of trade secrets relating to corn germplasm from one company by another – has nothing to do with "foreign intelligence." That information was not "necessary to . . . the ability of the United States to protect against . . . clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power," the only definition of "foreign intelligence information" that the government could possibly claim applies here. 50 U.S.C. § 1801(e)(1)(C).

The government's "foreign intelligence information" certifications thus appear to be clearly erroneous, and the "statement of the basis for the certification that . . . the information sought is the type of foreign intelligence information designated" likely contains material falsehoods and omissions. As with the government's assertions concerning the surveillance target's alleged status as a "foreign power" or an "agent of a foreign power," however, defense counsel cannot identify specific falsehoods or omissions, or establish clear error, without access to the underlying applications.

3. Certifications Concerning Necessity.

The government's applications to the FISC certified that the purported foreign intelligence information sought "cannot reasonably be obtained by normal investigative techniques."[7] The certifications included "a statement of the basis for the certification that . . . such [foreign intelligence] information cannot reasonably be obtained by normal investigative

[6] *Id.* § 1804(a)(6)(D), (E)(i).

[7] *Id.* § 1804(a)(6)(C).

techniques."[8] In his FISA suppression motion, Mr. Mo contends that the certifications were clearly erroneous, given the numerous other investigative techniques available to (and used by) the government, and that the "statements" likely contained material falsehoods and omissions.

In the Title III context, defendants have successfully challenged such statements of necessity for electronic surveillance under *Franks*. *See, e.g., United States v. Blackmon*, 273 F.3d 1204, 1208-10 (9th Cir. 2001); *United States v. Carneiro*, 861 F.2d 1171, 1180-82 (9th Cir. 1988); *United States v. Aileman*, 986 F. Supp. 1228, 1271 (N.D. Cal. 1997). Those challenges have succeeded because defense counsel have received access to the underlying wiretap applications and – based on their knowledge of the investigation – have been able to identify specific respects in which the statements of necessity have been false or materially incomplete. Given the implausibility of the government's necessity certifications here, disclosure of the underlying FISA materials to the defense will likely give rise to a similar challenge – and thus will substantially promote an accurate determination of the "necessity" issue.

* * * *

The "chameleon-like" word "necessary" in 50 U.S.C. § 1806(f) draws meaning from its context. The context here – particularly the legislative history of FISA and the statutory purpose to balance civil liberties and national security – shows that disclosure of FISA materials is "necessary" when it will substantially promote the accuracy of the court's determination of the legality of the surveillance. For the reasons outlined above, disclosure here plainly meets that standard.

---

[8] *Id.* § 1804(a)(6)(E)(ii).

II. DISCLOSURE OF THE FISA MATERIALS IS REQUIRED AS A MATTER OF DUE PROCESS.

If the Court declines to order production of the FISA applications, orders, and related materials under § 1806(f), then it should find that Mr. Mo is entitled to disclosure under § 1806(g) and the Fifth Amendment Due Process Clause.[9]

To determine whether due process requires the requested disclosure, the Court must consider the three factors set forth in *Mathews v. Eldridge*, 424 U.S. 319 (1976): (1) "the private interest that will be affected by the official action," (2) "the risk of an erroneous deprivation of such interest through the procedures used" and "the probable value, if any, of additional or substitute procedural safeguards," and (3) "the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirements would entail." *Id.* at 335; *see, e.g., American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1068-71 (9th Cir. 1995) (applying *Mathews* test to determine whether use of secret evidence violates due process); *Rafeedie v. INS*, 880 F.2d 506, 524-25 (D.C. Cir. 1989) (*Mathews* balancing test governs process due alien in exclusion proceeding, including use of secret evidence), *on remand*, 795 F. Supp. 13, 18-20 (D.D.C. 1992) (same); *Kiareldeen v. Reno*, 71 F. Supp. 2d 402, 413-14 (D.N.J. 1999) (same). Application of the *Mathews* test confirms that Mr. Mo must be granted access to the FISA materials as a matter of due process. The *Brady* due process analysis similarly requires disclosure.

A. The "Private Interest."

Mr. Mo's "private interests" here are extremely weighty. He seeks an accurate determination of his claim that the government's secret surveillance violated his rights under

[9] Section 1806(g) provides in relevant part that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*." 50 U.S.C. § 1806(g) (emphasis added).

FISA and the Fourth Amendment. He seeks to vindicate his constitutionally protected right to privacy. More generally, he seeks through the processes of this Court to avoid deprivation of his liberty. If mere property interests "weigh heavily in the *Mathews* balance," as the Supreme Court has held, *United States v. James Daniel Good Real Property*, 510 U.S. 43, 54-55 (1993), Mr. Mo's privacy and liberty interests have even greater significance.

B. The Risk of Erroneous Deprivation and the Value of Additional Procedures.

Turning to the second *Mathews* factor, the procedure that the government presumably will ask this Court to adopt – the adjudication of Mr. Mo's rights under FISA through *ex parte* review of materials that Mr. Mo's counsel will have no opportunity to examine or challenge – carries a notoriously significant "risk of an erroneous deprivation" of the liberty interests at issue, and "additional . . . procedural safeguards" – access to the FISA materials and an opportunity to address them – carry substantial "probable value." *Mathews*, 424 U.S. at 335. The Supreme Court has declared that "'[f]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.'" *James Daniel Good*, 510 U.S. at 55 (quoting *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170-72 (1951) (Frankfurter, J., concurring)). As the Ninth Circuit observed in a secret evidence case, "'One would be hard pressed to design a procedure more likely to result in erroneous deprivations.' . . . [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." *American-Arab Anti-Discrimination Committee*, 70 F.3d at 1069 (quoting district court); *see, e.g., id.* at 1070 (noting "enormous risk of error" in use of secret evidence); *Kiareldeen*, 71 F. Supp. 2d at 412-14 (same).

In the Fourth Amendment context, the Supreme Court has twice rejected the use of *ex parte* proceedings on grounds that apply equally here. In *Alderman v. United States*, 394 U.S. 165 (1969), the Court addressed the procedures to be followed in determining whether government eavesdropping in violation of the Fourth Amendment contributed to its case against the defendants. The Court rejected the government's suggestion that the district court make that determination *ex parte* and *in camera*. The Court observed that

> [a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances.

Id. at 182. In ordering disclosure of improperly recorded conversations, the Court declared:

> Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny that the Fourth Amendment exclusionary rule demands.

Id. at 184.

Similarly, the Court held in *Franks* that a defendant must be permitted to attack the veracity of the affidavit underlying a search warrant, upon a preliminary showing of an intentional or reckless material falsehood. The Court rested its decision in significant part on the *ex parte* nature of the procedure for issuing a search warrant and the value of adversarial proceedings:

> [T]he hearing before the magistrate [when the warrant is issued] not always will suffice to discourage lawless or reckless misconduct. The pre-search proceeding is necessarily ex parte, since the subject of the search cannot be tipped off to the application for a warrant lest he destroy or remove evidence. The usual reliance of our legal system on adversary proceedings itself should be an indication that an ex parte inquiry is likely to be less vigorous. The magistrate has no acquaintance with the information that may contradict the good faith and reasonable basis of the affiant's allegations. The pre-search proceeding will frequently be marked by

> haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an independent examination of the affiant or other witnesses.

438 U.S. at 169.

The same considerations that the Supreme Court found compelling in *Alderman* and *Franks* militate against *ex parte* procedures in the FISA context. As the FISC itself has acknowledged, for example, without adversarial proceedings, systematic executive branch misconduct – including submission of dozens of FISA applications with "erroneous statements" and "omissions of material facts" – went entirely undetected by the courts until the DOJ chose to reveal it. *See In re All Matters*, 218 F. Supp. 2d 611, 620-21 (Foreign Intelligence Surveillance Court), *rev'd*, 310 F.3d 717 (Foreign Intelligence Surveillance Court of Review 2002).[10] In light of the almost complete exclusion of criminal defendants and their counsel from the FISA review process, and the correspondingly low risk that misconduct will be detected, it is understandable, if inexcusable, that law enforcement officials "engaged in the often competitive enterprise of ferreting out crime," *Johnson v. United States*, 333 U.S. 10, 14 (1948), may have come to believe that FISA offers a convenient means of circumventing the traditional Title III and search warrant processes.

Three stark statistics underscore the dysfunction of the current FISA system: (1) year in and year out, the FISC approves without modification the overwhelming majority of the FISA applications the government presents and rejects only a tiny handful – if that – out of more than a

[10] The FISC was sufficiently alarmed by these erroneous applications that it "decided not to accept inaccurate affidavits from FBI agents whether or not intentionally false," and "[o]ne FBI agent was barred from appearing before the Court as a FISA affiant." *In re All Matters*, 218 F. Supp. 2d at 621.

thousand;[11] (2) no court has ever granted defense counsel access to FISA applications and orders under § 1806(f), so no adversarial eye has ever scrutinized them; and (3) no court has ever granted a motion to suppress the fruits of FISA surveillance.

As these statistics suggest, *ex parte* review under the "minimal scrutiny" standard that FISA contemplates does not adequately protect the surveillance target's constitutional and statutory rights. The "additional . . . procedural safeguards" that Mr. Mo requests – access to the FISA materials and an opportunity to address them – thus carry substantial "probable value." *Mathews*, 424 U.S. at 335.

C. The Government's Interest.

Finally, the Court must consider the government's purported interest in maintaining the secrecy of the FISA materials. We expect the government to assert its generalized interest in avoiding damage to "national security," without any effort to demonstrate that disclosure of the FISA materials to defense counsel under the circumstances of this case would cause such damage. Courts have previously rejected such diffuse claims of national security. *See, e.g., Arab-American Anti-Discrimination Committee*, 70 F.3d at 1070 ("We cannot in good conscience find that the President's broad generalization regarding a distant foreign policy concern and a related national security threat suffices to support a process that is inherently unfair because of the enormous risk of error and the substantial personal interests involved."); *Kiareldeen*, 71 F. Supp. 2d at 414 (same); *Rafeedie*, 795 F. Supp. at 19 (same).

---

[11] According to the Attorney General's annual reports (available at http://fas.org/irp/agency/doj/fisa), since 1978 the FISC has approved (either as submitted or with modifications) well over 20,000 applications or extensions authorizing FISA surveillance, more than 99% of the total applications submitted. The FISC has rejected outright only a handful of applications, and the DOJ has successfully resubmitted some of those. The statistics for 2013 are typical: the government made 1,588 applications for electronic surveillance; none were denied or withdrawn; and the FISC modified 34 applications.

The government's asserted national security interest in withholding the FISA materials from the defense is particularly weak here in light of the protections available under CIPA. Most critically, CIPA provides for entry of a protective order.[12] The CIPA protective order – the standard terms of which are largely settled after decades of experience – sets the conditions under which defense counsel may review classified discovery, establishes procedures for filing classified pleadings, and prohibits anyone associated with the defense from revealing publicly the classified information to which access is granted. *See, e.g., United States v. Gowadia*, 2010 U.S. Dist. LEXIS 80572 (D. Haw. May 8, 2010) (entering a typical CIPA protective order).

The protective order also appoints Court Security Officers in accordance with the security procedures adopted by the Chief Justice under CIPA § 9(a).[13] Although the CSOs work for the Department of Justice, they are independent of the prosecution team. They advise the parties and the court on the proper handling of classified information, and they serve as conduits for the flow of classified discovery and pleadings among the parties and the Court.[14]

The CIPA protective order requires defense counsel and other members of the defense team to obtain security clearances before receiving access to classified discovery.[15] The protective order also requires the defense to maintain all classified information in a Sensitive Compartmented Information Facility, or SCIF. The SCIF consists of one or more secure rooms, usually in the federal courthouse where the case is being heard. It is protected by locks and other

---

[12] 18 U.S.C. App. 3 § 3.

[13] 18 U.S.C. App. 3 § 9(a). The procedures, issued by Chief Justice Warren Burger in 1981, appear in a note following CIPA § 9.

[14] *See* 9 United States Attorney's Manual, Criminal Resource Manual § 2054(I)(C) (describing role of CSO).

[15] Mr. Mo's defense counsel are prepared to seek security clearances as soon as the protective order is in place and a CSO is appointed.

security devices. The SCIF contains safes to hold classified documents, secure computers on which to prepare classified pleadings, and other approved equipment.

Once the protective order is in place, defense counsel has the necessary clearance, and the SCIF is ready, the parties begin the classified discovery process. CIPA § 4 governs classified discovery. That provision allows the court to authorize the government, "upon a sufficient showing," to delete classified information from the discovery it provides or to furnish substitutions for the classified information in the form of summaries or admissions. The statute adds that "[t]he court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone." 18 U.S.C. App. 3 § 4.

CIPA has been in existence more than 34 years. During that time huge volumes of enormously sensitive classified information have been made available under its strict security measures to cleared defense counsel in scores of federal criminal cases – without, as far as counsel are aware, a serious security violation by the defense. In one case, for example, the CIPA procedures successfully protected nuclear weapon codes that government scientists testified under oath were capable of "changing the strategic global balance" and thus "represent[ed] the gravest possible security risk to the United States." *United States v. Lee*, 2000 U.S. App. LEXIS 3082, at *5-*6 (10th Cir. Feb. 29, 2000). If the CIPA procedures could adequately protect those secrets (and other sensitive classified information in many other cases), they can surely protect the secrets contained in the FISA materials at issue here. In short, CIPA provides precisely the "appropriate security procedures and protective orders" that Congress contemplated would accompany disclosure when it enacted FISA. 50 U.S.C. § 1806(f).

We urge the Court to view the government's claimed need for secrecy – and to evaluate the third *Mathews* factor – in light of previous, similar national security claims that have proven

exaggerated. To cite a few famous examples, the government argued in 1971 that disclosure of the Pentagon Papers would cause grave damage national security. *See New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam). The New York Times published the Papers, and there is no evidence that national security suffered in the slightest. In 1979, the government sought to suppress Howard Morland's article, The H-Bomb Secret, claiming that publication would cause immediate and irreparable harm to national security. *See United States v. Progressive, Inc.*, 486 F. Supp. 5 (D. Wis.), *dismissed as moot*, 610 F.2d 819 (7th Cir. 1979). The Progressive published Morland's article in November 1979, and – again – there is no evidence of any harm to national security. In December 1999, the government made strident national security claims to convince a federal court to detain Dr. Wen Ho Lee under extraordinarily strict conditions for nine months. *See United States v. Lee*, 79 F. Supp. 2d 1280 (D.N.M. 1999), *aff'd mem.*, 208 F.3d 228 (10th Cir. 2000). In September 2000, following a plea bargain, Dr. Lee regained his freedom. There is no evidence that his release has caused any damage to the national security.

These examples (and many others) share several common features: in each case, the government invoked national security to convince a court to depart from constitutional standards; in each case, courts initially acceded to the government's national security claims; and in each case, when the "doomsday" event actually occurred, the government's purported concerns proved unfounded. As the Fourth Circuit has observed in the First Amendment context:

> History teaches us how easily the spectre of a threat to "national security" may be used to justify a wide variety of repressive government actions. A blind acceptance by the courts of the government's insistence on the need for secrecy, without notice to others, without argument, and without a statement of reasons, would impermissibly compromise the independence of the judiciary and open the door to possible abuse.

In re Washington Post Co., 807 F.2d 383, 391-92 (4th Cir. 1986). In accordance with *Washington Post*, we ask the Court, when applying the third *Mathews* factor, to scrutinize with an independent eye the government's claim that disclosure of the FISA materials, under the particular circumstances of this case and with all the protections CIPA affords, will damage national security. Upon an objective assessment of that claim, the Court should find that the first and second Mathews factors substantially outweigh the government's professed need to withhold the FISA materials from defense counsel.

D. Disclosure Is Also Required Under *Brady*.

Brady requires production of material evidence that would be favorable to the defendant on a motion to suppress. *See United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000) ("The suppression of material evidence helpful to the accused, *whether at trial or on a motion to suppress*, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different.") (emphasis added). For the reasons we have outlined, the FISA applications and other materials are helpful to the defense in preparing the motion to suppress the FISA-derived evidence. *Brady* thus requires their disclosure.

CONCLUSION

More than fifty years ago, the Supreme Court declared that "since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense." *Jencks v. United States*, 353 U.S. 657, 671 (1957) (quotation omitted); *see, e.g., United States v. Reynolds*, 345 U.S. 1, 12 (1953); *United States v. Andolschek*, 142 F.2d 503, 506 (2d Cir. 1944).

The government has charged Mr. Mo with conspiracy to steal trade secrets, a serious felony; it proposes to use against him at trial evidence derived from FISA surveillance; but it wants to withhold from him information that is material to his contention that the government obtained the FISA evidence in violation of the statute and his Fourth Amendment rights. *Jencks* and its progeny prohibit the prosecution from "invok[ing] its governmental privileges" in this manner. In accordance with 50 U.S.C. § 1806(f) and the Fifth Amendment Due Process Clause, the Court should order disclosure of the FISA applications, orders, and related materials to defense counsel, under the procedures outlined in CIPA.

WEINHARDT & LOGAN, P.C.

By _____
Mark E. Weinhardt AT0008280
Holly M. Logan AT0004710

2600 Grand Avenue, Suite 450
Des Moines, IA 50312
Telephone: (515) 244-3100
E-mail: mweinhardt@weinhardtlogan.com
hlogan@weinhardtlogan.com

LAW OFFICE OF MARK BECK

By _____
Mark Beck (Admitted pro hac vice)

350 West Colorado Blvd, Suite 200
Pasadena, CA 91105
Telephone: (626) 234-5334
Email: mbeck@markbecklaw.com
ATTORNEYS FOR MO HAILONG, ALSO KNOWN AS ROBERT MO

PROOF OF SERVICE

The undersigned certifies that the foregoing instrument was served upon the parties to this action by serving a copy upon each of the attorneys listed below on March 13, 2015, by

- ☐ U.S. Mail
- ☐ FAX
- ☐ Hand Delivered
- ☐ Electronic Mail
- ☐ FedEx/ Overnight Carrier
- ☒ CM / ECF

Jason T. Griess
U.S. Attorney's Office
jason.griess2@usdoj.gov

Marc Krickbaum
marc.krickbaum@usdoj.gov

Leon F. Spies
Mellon & Spies
Spieslegal@aol.com

Terry W. Bird
Bird Marella
TWB@birdmarella.com

ATTORNEYS FOR MO YUN

Signature: N Baldus